METHOD AND APPARATUS FOR PROVIDING INFORMATION SECURITY TO PREVENT DIGITAL SIGNATURE FORGERY

Abstract Of The Disclosure

A method and apparatus utilizes a digital signature verification map containing a plurality of acceptable message header identifiers associated with a public key certificate identifier. In one embodiment, a method includes determining a digital signature verification error based on a received message header, such as transport header identifier associated with a public key certificate identifier, such as the subject field of the certificate. The method includes generating a signature verification map or updating a signature verification map containing a plurality of acceptable message header identifiers associated with the common public key certificate identifier in response to determining the digital signature verification error. Accordingly, a link is provided between a transport header and a digitally signed message. A digital signature verification map is continually updated to accommodate aliases to a common subject associated with the certificate. The digital signature verification map is preferably digitally signed to maintain a trusted verification map to operate as part of a secure communication system. If desired, a trusted alias map may also be used.